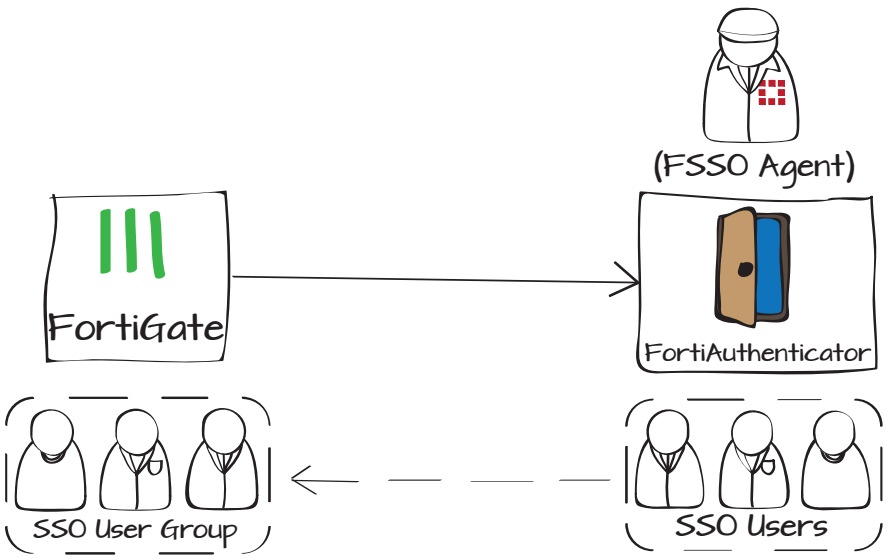
Allowing Single Sign-On access with a FortiGate and a FortiAuthenticator

This example illustrates how to configure Single Sign-On (SSO) using a FortiGate and FortiAuthenticator, with the FortiAuthenticator unit acting as the SSO Agent, verifying and maintaining user login information. Users can then log in once when connecting to the internal network behind the FortiGate, and be automatically logged into servers and services that support SSO.

1. Configuring polling on the FortiAuthenticator
2. Adding a FortiAuthenticator to the FortiGate unit
3. Creating the FSSO user group
4. Creating a security policy
5. Results



Configuring polling on the FortiAuthenticator

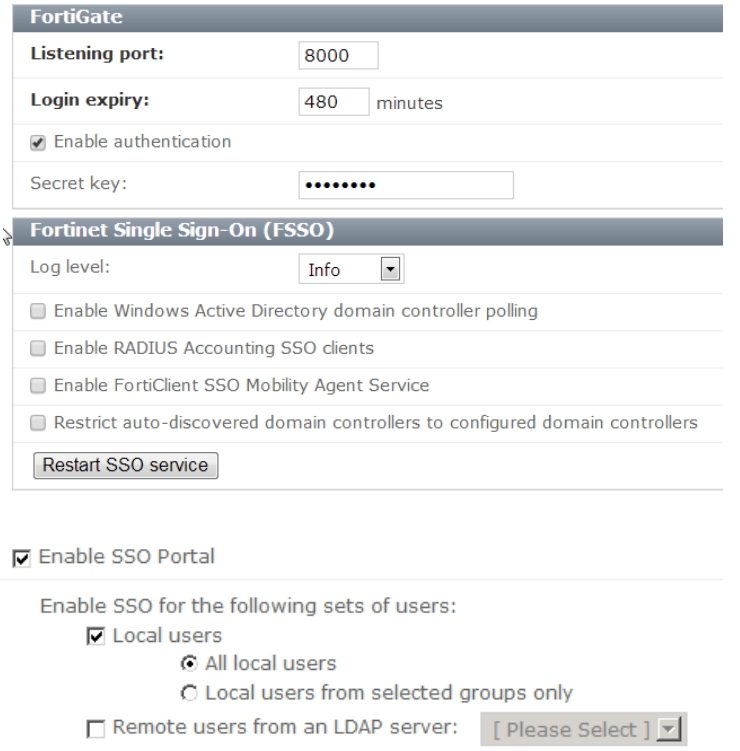
In the FortiAuthenticator interface, go to **SSO & Dynamic Policies > SSO > Options**.

In the **FortiGate** section, the Listening Port should be 8000, unless the FortiGate's default port mapping has been changed.

Select **Enable Authentication**. and enter the **Secret Key**, which you will use when configuring the FSSO Agent on the FortiGate.

If you are using an external SSO service, such as Windows AD or a remote LDAP server, enable it in the the **Fortinet Single Sign-On (FSSO)** section.

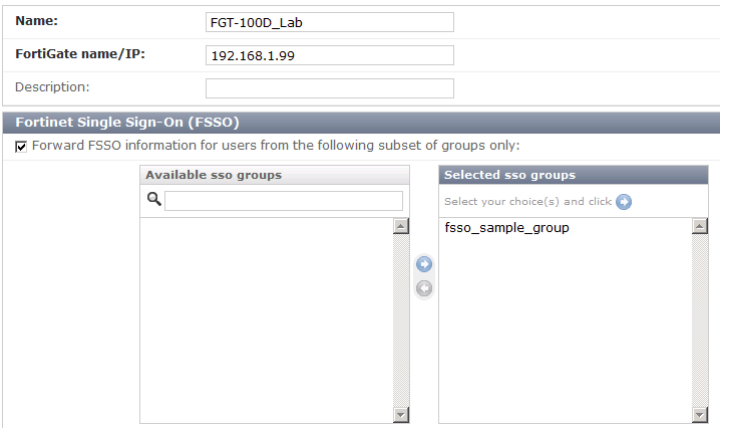
Go to **SSO & Dynamic Policies > SSO > Login Portal** and **Enable SSO Portal**. Ensure **Local users** is enabled, and disable **Remote users from an LDAP server**.



Then go to **SSO & Dynamic Policies > SSO > FortiGate Group Filtering**.

Create a new **FortiGate Group Filter**, entering the FortiGate's IP/hostname.

Enable **Forward FSSO information for users from the following subset of groups only** and move the groups you'd like to send to the FortiGate from **Available** to **Selected**. Select **OK** to save the filter.



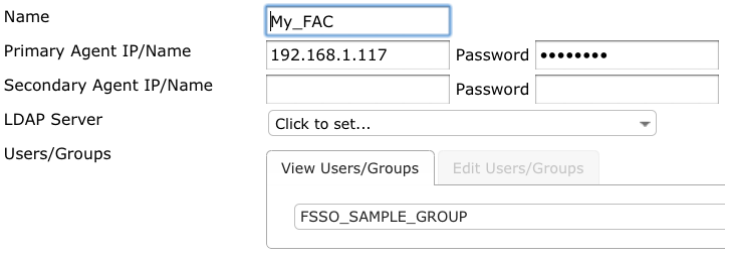
Adding a FortiAuthenticator to the FortiGate unit

In the FortiGate interface, go to **User & Device > Authentication > Single Sign-On**, and select **Create New**.

For the **Type**, select Fortinet Single Sign-On Agent. Enter a **Name** for the FortiAuthenticator unit.

Enter the IP address of the FortiAuthenticator as the **Primary Agent IP/Name**, and enter the secret key as the **Password**.

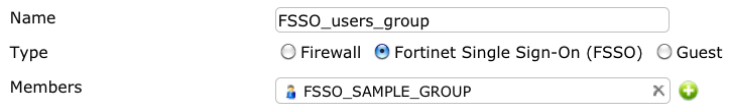
Select **Apply & Refresh**, and wait a minute for the FortiAuthenticator to connect to the FortiGate and download user group information.



Creating the FSSO user group

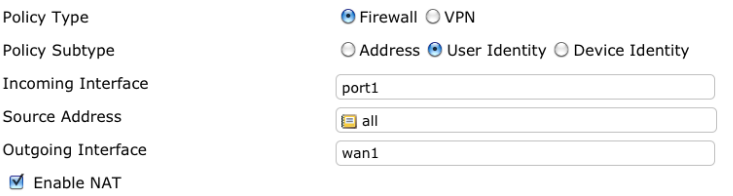
You cannot directly use the user groups imported from FortiAuthenticator in firewall policies, so you will need to create FortiGate user groups to represent the FortiAuthenticator groups. Go to **User & Device > User > User Groups**, and create a new FSSO user group.

The **Members** list will be populated with the FortiAuthenticator's user groups. Select the imported groups to add them to the FortiGate group's **Members** list.

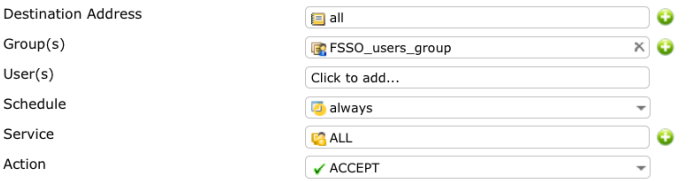


Creating a security policy

Now, create a security policy to handle SSO user traffic, so it can be easily identified in logs and reports. Go to **Policy > Policy > Policy**, and create a new policy, setting the **Policy Subtype** to **User Identity**.



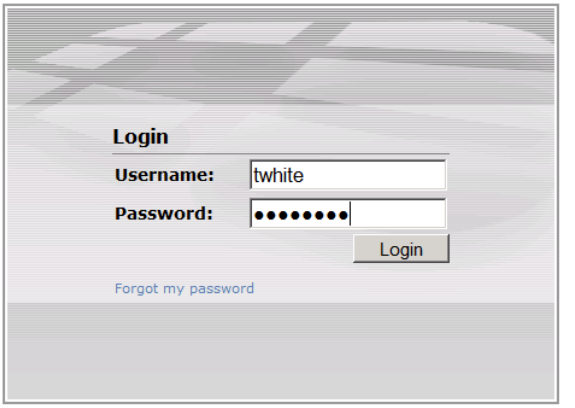
Multiple **Authentication Rules** can be created for different groups of SSO users that require different access and supervision.



Results

With the identity-based policy being the only policy connecting the internal network to the internet, users on the internal network will not be able to access the internet without authenticating.

To connect to the internet, users must navigate in a browser to the FortiAuthenticator's IP. Users will then log into the FortiAuthenticator as an admin would, but will only have access to their user account settings in the FAC interface.



Once the user has logged in, the FortiAuthenticator retains their user information for a time specified in the SSO Portal settings. They will have access to the internet, and to any other services or servers on the internal network configured to use SSO with the FortiAuthenticator.